Sapphire/Slammer

The Fastest Worm Yet

Stuart Staniford

Silicon Defense

www.silicondefense.com

Collaborators

David Moore, CAIDA and UC San Diego

Vern Paxson, ICSI

Stefan Savage, UC San Diego

Colleen Shannon, CAIDA

Stuart Staniford, Silicon Defense

Nicholas Weaver, UC Berkeley and Silicon Defense

SILICON DEFENSE

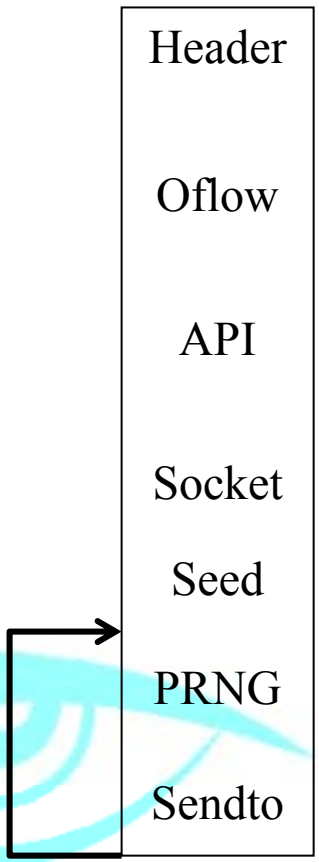
Impact of Sapphire

- Major ATM network down for most of a day
- 911 service in a major city lost
- Disruption of provincial elections in Canada
- Numerous companies with network out of control for 1-3 days (but many fine)
- Parts of Internet congested for about 12 hours.
- Overall, moderate disruption.
- But worst worm incident to date

SILICON DEFENSE

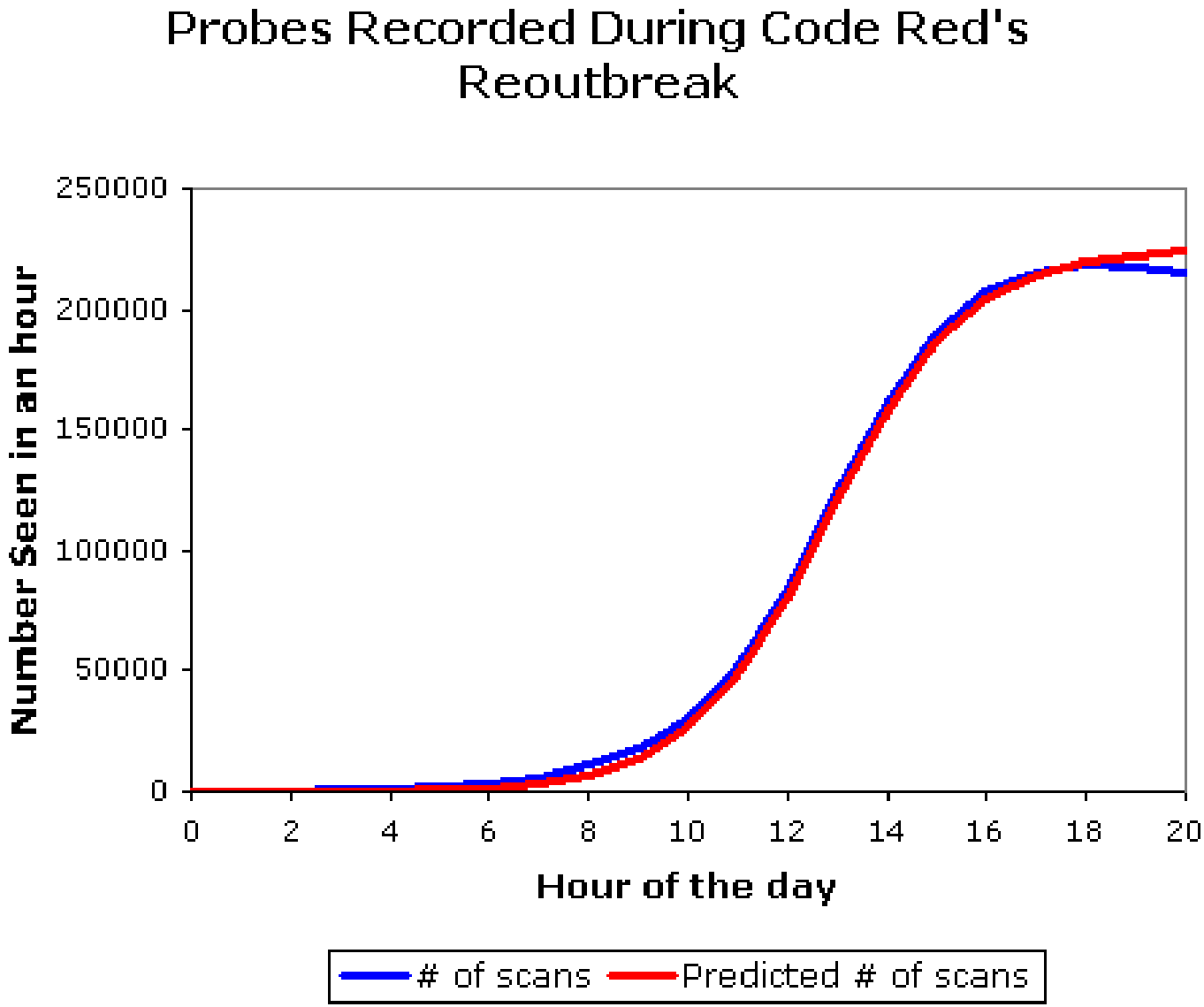
What Was Sapphire?

- Sapphire was a worm in one UDP packet
- 404 bytes total
- Microsoft SQL vulnerability
- Spewed packets at high speed
- Didn't need response
- Spread very fast
  - globally in 10 mins



SILICON DEFENSE

Random Scanning Worms



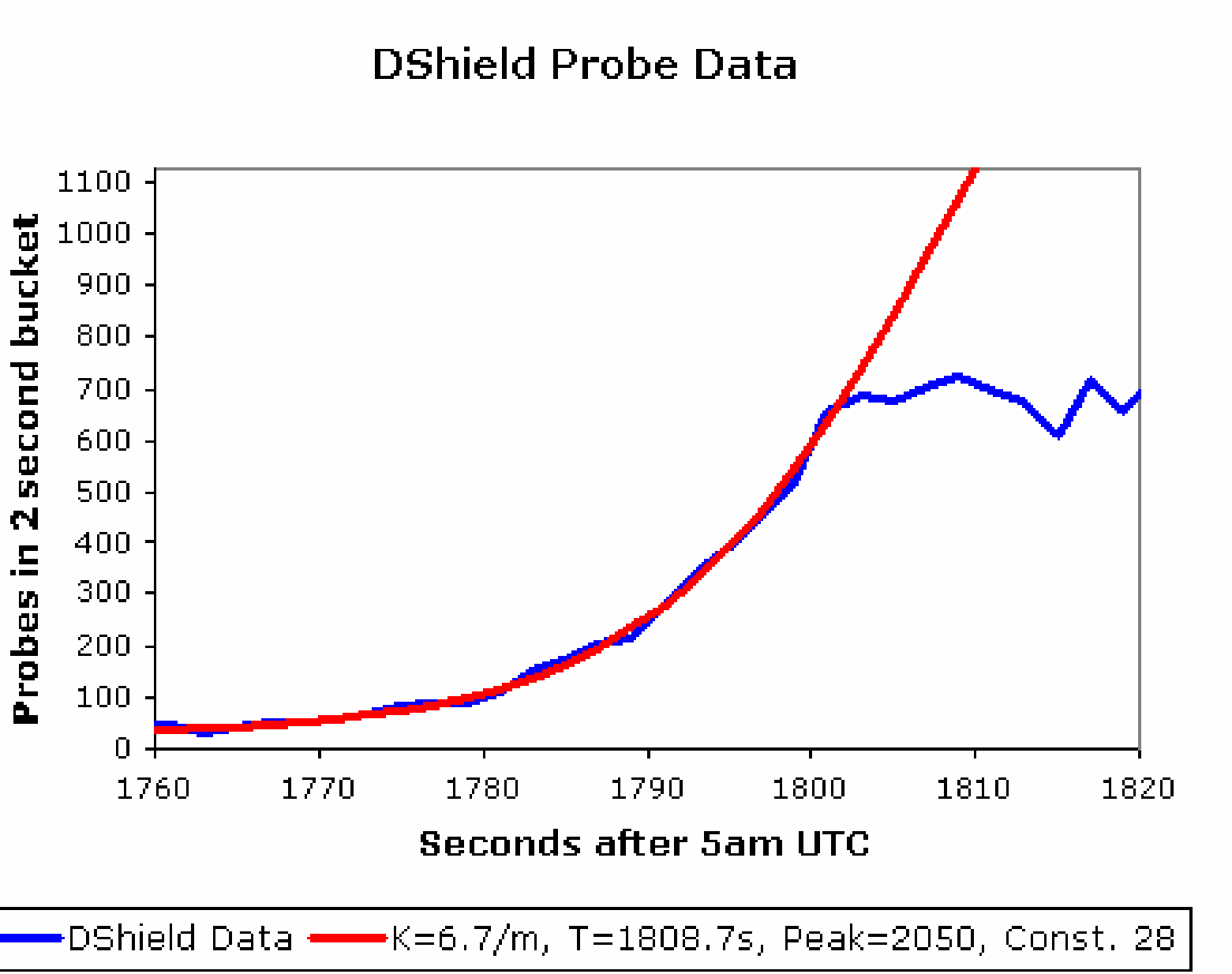
SILICON DEFENSE

Random Scanning Worms II

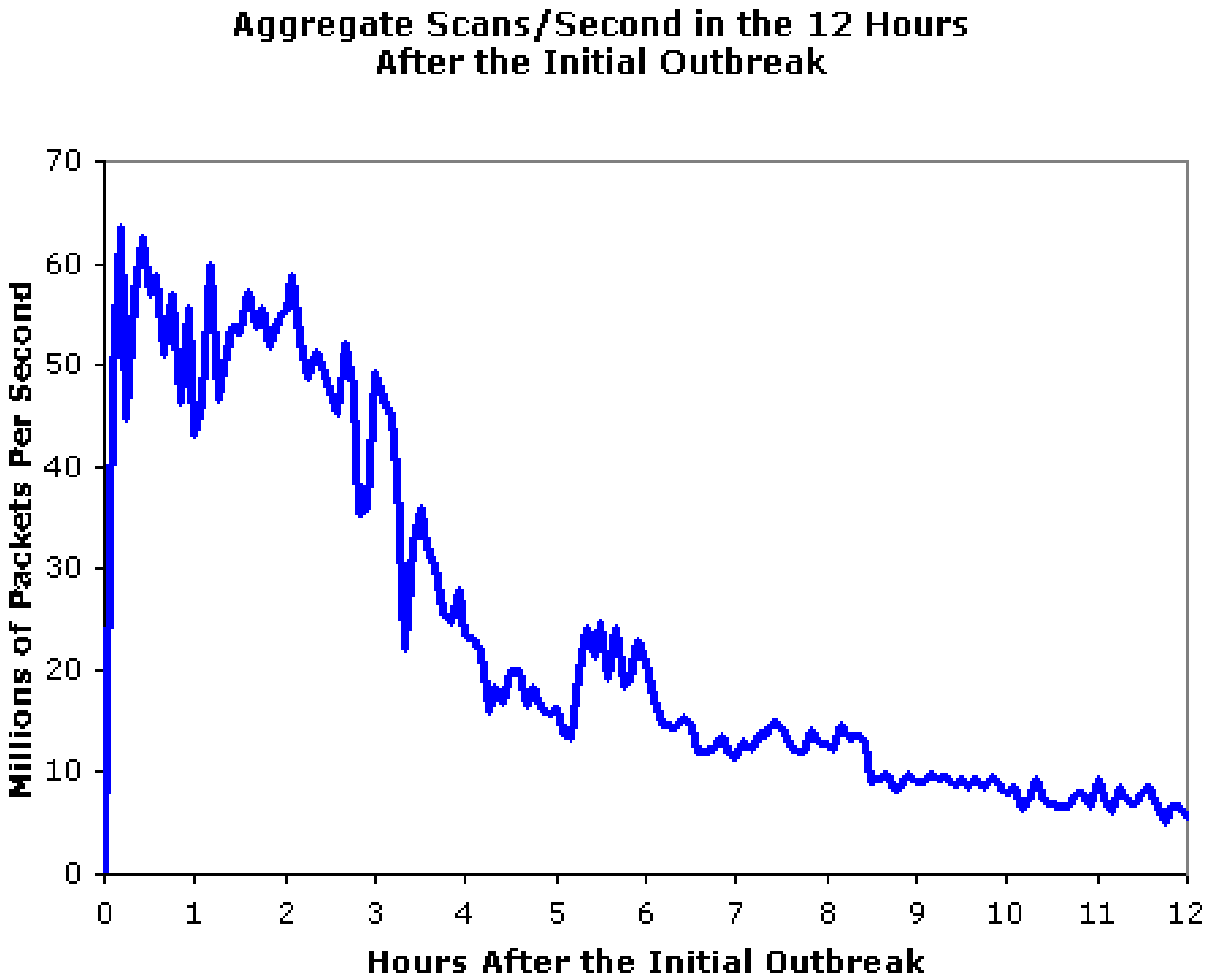
- Simple scanning worm dynamics
- $a = e^{vS(t-T)} / (1+e^{vS(t-T)})$
- a is proportion infected
- t is time
- Gives sigmoidal graph centered on T
- v is effective vulnerability density (8×10^{-5} for CRI)
- S is effective scan rate (6.25/s for CRI)

SILICON DEFENSE

Sapphire Spread Speed

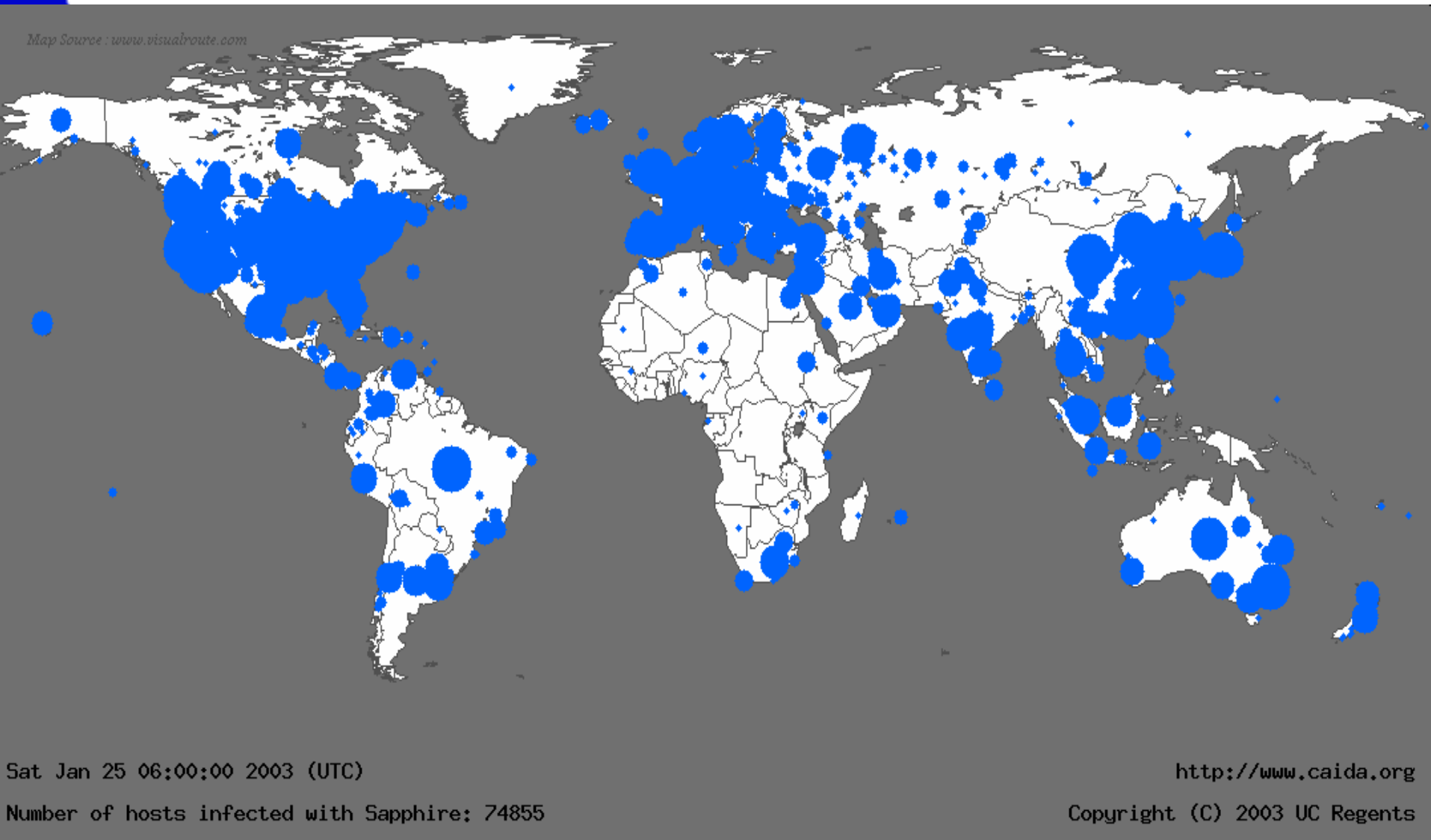


Scan Rates and Response



SILICON DEFENSE

Geographical Spread



Geographical Spread II

Country	% Victims	TLD	% Victims
United States	42.87	UNKNOWN	59.49
South Korea	11.82	net	14.37
UNKNOWN	6.96	com	10.75
China	6.29	edu	2.79
Taiwan	3.98	tw	1.29
Canada	2.88	au	0.71
Australia	2.38	ca	0.71
United Kingdom	2.02	jp	0.65
Japan	1.72	br	0.57
Netherlands	1.53	uk	0.57

SILICON DEFENSE

Random Number Generator

- Has defects due to coding errors
- Has cycle structure
  - Each worm copy will stay within initial cycle
  - Cycles amongst certain /16 addresses - doesn't visit all.
  - Several different cycle structures depending on exact version of SQL server
- Therefore hard to count how many Ips infected
- >75000

SILICON DEFENSE

Conclusions

- Sapphire was fastest worm ever
- Speed prediction (How to 0wn..): accurate
- Worms can spread in minutes (even RS)
- RS worms can live on smaller vulnerable populations than we realized
  - <20000 on the Internet would be ample to support sub-hour spread
- Can work on TCP (but harder to implement)

SILICON DEFENSE

Conclusions II

- Surprising level of disruption for a no-payload, no-firewall-penetrator worm.
- Worm with the above could be devastating
- Need automated defenses

SILICON DEFENSE